PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-149611
(43)Date of publication of application : 24.05.2002

(51)Int.Cl. G06F 15/00
G06F 17/60
H04L 9/32

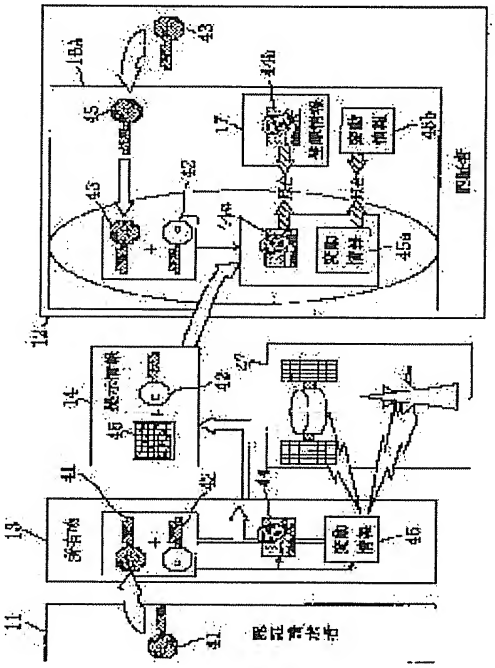
(21)Application number : 2001-259436
(22)Date of filing : 29.08.2001

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : ODAKAWA AKIHIRO

(30)Priority
Priority number : 2000260390 Priority date : 30.08.2000 Priority country : JP

(54) AUTHENTICATION SYSTEM, AUTHENTICATION REQUESTING DEVICE, VERIFICATION DEVICE AND SERVICE MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an authentication system for reducing the fear of appropriation of the third person and an authentication requesting device, a verification device and a service medium which are to be used for the authentication system.
SOLUTION: An authentication requesting person 11 requests authentication by using his/her belongings 13. When a ciphering key 41 for requesting authentication is inputted to the belongings 13, the key 41 and a public key 42 (public information for preparing a cipher) are matched to calculate cipher information 46 from biometrics information 44 and variation information 45 on varying position, time, etc., to be sent to a verification part 16A as presenting information 14. The part 16A decodes cipher information 46 by using a cipher key 43 for authentication and the public key 42 (public information for preparing a cipher) to collate information. The key 41 is constituted so as to only flow through inside of the belonging and the part 16A and to avoid remaining as a default value, thereby the fear of appropriation of the key 41 by the third party is reduced.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－149611
（P2002－149611A）
(43)公開日　平成14年５月24日(2002.5.24)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｅ	５Ｂ０８５
	17/60	２２２	17/60	２２２	５Ｊ１０４
		４１４		４１４	
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ　9/00	６７３Ｃ	
				６７５Ａ	

審査請求　有　請求項の数22　ＯＬ　（全 19 頁）

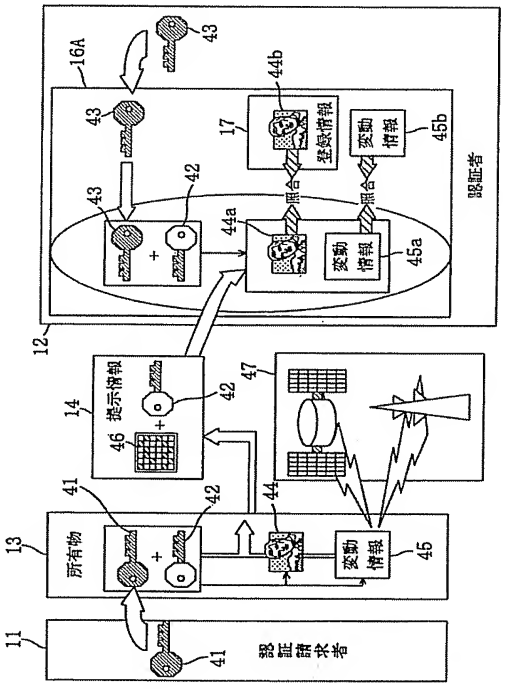
(21)出願番号　特願2001－259436(P2001－259436)
(22)出願日　平成13年８月29日(2001.8.29)
(31)優先権主張番号　特願2000－260390(P2000－260390)
(32)優先日　平成12年８月30日(2000.8.30)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　小田川　明弘
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100077931
弁理士　前田　弘　（外７名）

Ｆターム(参考)　5B085 AE09 AE23
5J104 AA07 KA01 KA04 KA05 NA02
NA05

(54)【発明の名称】　認証システム，認証請求装置，検証装置及びサービス媒体

(57)【要約】
【課題】　第三者の盗用のおそれを低減するための認証システム及び認証システムに用いられる認証請求装置，検証装置及びサービス媒体を提供する。
【解決手段】　認証請求者１１は、その所有物１３を用いて認証を請求する。所有物１３に認証請求用の暗号鍵４１が入力されると、暗号鍵４１と公開鍵４２（暗号作成用公開情報）とが合わせられ、バイオメトリクス情報４４と、変動する位置，時間などに関する変動情報４５とから暗号情報４６が算出され、提示情報１４として検証部１６Ａに送られる。検証部１６Ａでは、認証用の暗号鍵４３と公開鍵４２（暗号解読用公開情報）とを用いて暗号情報４６がデコードされ、情報の照合が行われる。暗号鍵４１は所有物１３や検証部１６Ａ内を流通するだけで、デフォルト値として残らないように構成することにより、第三者が暗号鍵４１を盗用するおそれが低減される。



1

【特許請求の範囲】

【請求項１】　認証請求者からの請求に応じて、認証者が認証請求者の適格性を認証する際に用いられる認証システムであって、

上記認証請求者に固有の認証請求用の固定情報と、時間的に変動する特性を有する変動情報とを受け、上記認証請求用の固定情報と上記変動情報とに基づいて、暗号情報を作成する暗号情報作成手段と、

上記認証請求用の固定情報に対応する認証用の固定情報と、上記暗号情報とを受けて、上記暗号情報から少なくとも上記認証請求用の固定情報を復元する情報復元手段とを備えている認証システム。

【請求項２】　請求項１に記載の認証システムにおいて、

上記認証請求者に固有の認証請求用のもう１つの固定情報を記憶する第１の固定情報記憶手段と、

上記認証請求用のもう１つの固定情報に対応する認証用のもう１つの固定情報を記憶する第２の固定情報記憶手段とをさらに備え、

上記暗号作成手段は、上記認証請求用のもう１つの固定情報をも含めて上記暗号情報を作成し、

上記情報復元手段は、上記認証請求用のもう１つの固定情報をも復元することを特徴とする認証システム。

【請求項３】　請求項２に記載の認証システムにおいて、

上記情報復元手段及び上記もう１つの固定情報記憶手段の出力を受けて、上記認証請求用のもう１つの固定情報と上記認証用のもう１つの固定情報とを照合する照合手段をさらに備えていることを特徴とする認証システム。

【請求項４】　請求項３に記載の認証システムにおいて、

上記復元手段は、上記変動情報をも復元し、

上記復元された上記変動情報を受けて、変動情報に基づいて、認証請求者の適格性を判定する判定手段をさらに備えていることを特徴とする認証システム。

【請求項５】　請求項１～４のうちいずれか１つに記載の認証システムにおいて、

上記暗号情報作成手段は、暗号作成用の公開情報をも用いて上記暗号情報を作成し、

上記情報復元手段は、暗号解読用の公開情報をも用いて上記復元を行なうことを特徴とする認証システム。

【請求項６】　請求項１に記載の認証システムにおいて、

上記認証者が複数存在しており、

上記認証請求用の固定情報は、各認証者に対して共通化されていることを特徴とする認証システム。

【請求項７】　請求項１に記載の認証システムにおいて、

上記暗号情報作成手段と上記情報復元手段とは、１つの媒体に組み込まれており、

2

上記媒体は、音声信号及び映像信号のうち少なくともいずれか１つを生成するための回路と、

上記復元された上記認証請求用の固定情報を受けて、上記固定情報に基づいて、上記回路の作動・非作動を制御する制御手段とをさらに備えていることを特徴とする認証システム。

【請求項８】　認証請求者からの請求に応じて、認証者が認証請求者の適格性を認証する際に用いられる認証システムであって、

少なくとも時間的に変動する特性を有する変動情報を受け、上記変動情報に基づいて、暗号情報を作成する暗号情報作成手段と、

請求用の固定情報に対応する認証用の固定情報と、上記暗号情報とを受けて、

上記暗号情報から少なくとも上記変動情報を復元する情報復元手段とを備えている認証システム。

【請求項９】　請求項８に記載の認証システムにおいて、

上記変動情報の適否判定のための登録情報を記憶する登録情報記憶手段と、

上記登録情報に基づいて、上記復元された変動情報の適否を判定する適否判定手段とをさらに備えていることを特徴とする認証システム。

【請求項１０】　認証請求者からの請求に応じて、認証者が認証請求者の適格性を認証する際に用いられる認証システム中の認証請求装置であって、

時間的に変動する特性を有する変動情報を受ける変動情報入力部と、

上記変動情報入力部を受け、上記変動情報に基づいて、暗号情報を作成する暗号情報作成手段とを備えている認証請求装置。

【請求項１１】　請求項１０に記載の認証システムにおいて、

上記認証請求者に固有の認証請求用の固定情報を受ける固定情報入力部をさらに備え、

上記暗号情報作成手段は、上記固定情報と上記変動情報とに基づいて、上記暗号情報を作成することを特徴とする認証請求装置。

【請求項１２】　請求項１０又は１１に記載の認証請求装置において、

上記認証請求者に固有の認証請求用のもう１つの固定情報を記憶する第１の固定情報記憶手段と、

上記認証請求用のもう１つの固定情報に対応する認証用のもう１つの固定情報を記憶する第２の固定情報記憶手段とをさらに備え、

上記暗号作成手段は、上記認証請求用のもう１つの固定情報をも含めて上記暗号情報を作成することを特徴とする認証請求装置。

【請求項１３】　請求項１２に記載の認証請求装置において、

上記もう１つの固定情報は、認証請求者を識別する画像情報を基に作成されていることを特徴とする認証請求装置。

【請求項１４】　請求項１１～１３のうちいずれか１つに記載の認証請求装置において、
上記変動情報は、ＧＰＳ（グローバル・ポジショニング・システム）に基づいて設定されていることを特徴とする認証請求装置。

【請求項１５】　請求項１１～１３のうちいずれか１つに記載の認証請求装置において、
上記変動情報は、移動体情報端末および移動体基地局からの情報に基づいて設定されていることを特徴とする認証請求装置。

【請求項１６】　認証請求者からの請求に応じて、認証者が認証請求者の適格性を認証する際に用いられる認証システム中の検証装置であって、
認証請求者から送られる，認証請求者固有の認証請求用の固定情報と変動情報とに基づいて作成された暗号情報を受ける暗号情報入力部と、
上記認証請求用の固定情報に対応する認証用の固定情報を入力する固定情報入力部と、
上記暗号情報作成入力部及び固定情報入力部の出力を受けて、上記暗号情報から少なくとも上記認証請求用の固定情報を復元する情報復元手段とを備えている検証装置。

【請求項１７】　請求項１６に記載の検証装置において、
上記認証請求者から送られる暗号情報には、認証請求用の固定情報に対応する認証用のもう１つの固定情報が含まれており、
上記認証請求用のもう１つの固定情報に対応する認証用のもう１つの固定情報を記憶する固定情報記憶手段と、
上記情報復元手段及び上記固定情報記憶手段の出力を受けて、上記認証請求用のもう１つの固定情報と上記認証用の固定情報とを照合する照合手段とをさらに備えていることを特徴とする検証装置。

【請求項１８】　請求項１６又は１７に記載の検証装置において、
上記復元手段は、上記変動情報をも復元し、
上記復元された上記変動情報を受けて、変動情報に基づいて、認証請求者の適格性を判定する判定手段をさらに備えていることを特徴とする検証装置。

【請求項１９】　認証請求者からの請求に応じて、認証者が認証請求者の適格性を認証する際に用いられる認証システム中の検証装置であって、
認証請求者から送られる変動情報とに基づいて作成された暗号情報を受ける暗号情報入力部と、
上記暗号情報作成入力部の出力を受けて、上記暗号情報から少なくとも上記変動情報を復元する情報復元手段とを備えている検証装置。

【請求項２０】　請求項１９に記載の検証装置において、
上記変動情報の適否判定のための登録情報を記憶する登録情報記憶手段と、
上記登録情報に基づいて、上記復元された変動情報の適否を判定する適否判定手段とをさらに備えていることを特徴とする検証装置。

【請求項２１】　認証請求者からの請求に応じて、認証者が認証請求者の適格性を認証する際に用いられる認証システム中のサービス媒体であって、
上記認証請求者に固有の認証請求用の固定情報を受ける固定情報入力部と、
時間的に変動する特性を有する変動情報を受ける変動情報入力部と、
上記認証請求用の固定情報と上記変動情報とを受け、上記認証請求用の固定情報と上記変動情報とに基づいて、暗号情報を作成する暗号情報作成手段と、
上記認証請求用の固定情報に対応する認証用の固定情報と、上記暗号情報作成手段の出力とを受けて、上記暗号情報から少なくとも上記認証請求用の固定情報を復元する情報復元手段と、
音声信号及び映像信号のうち少なくともいずれか１つを生成するための回路と、
上記復元された上記認証請求用の固定情報を受けて、上記固定情報に基づいて、上記回路の作動・非作動を制御する制御手段とを備えているサービス媒体。

【請求項２２】　認証請求者からの請求に応じて、認証者が認証請求者の適格性を認証する際に用いられる認証システム中のサービス媒体であって、
時間的に変動する特性を有する変動情報を受ける変動情報入力部と、
上記変動情報に基づいて、暗号情報を作成する暗号情報作成手段と、
上記暗号情報作成手段の出力を受けて、上記暗号情報から少なくとも上記変動情報を復元する情報復元手段と、
音声信号及び映像信号のうち少なくともいずれか１つを生成するための回路と、
上記復元された上記変動情報を受けて、上記変動情報に基づいて、上記回路の作動・非作動を制御する制御手段とを備えているサービス媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、サービスや商品の提供を受ける際に利用することができる認証システム，その認証請求装置，検証装置及びサービス媒体に関するものである。

【０００２】

【従来の技術】従来より、サービスや商品の提供を受ける際に、その提供を受けることを請求する者が提供を受ける適格性を有する者であるか否かを判定するための認

5

証が行なわれている。以下、認証が利用される幾つかの例を具体的に挙げる。

【０００３】◎認証認証の代表例として銀行の預金システムを考える場合、利用者は銀行に自分の口座開設を依頼する。この口座開設は、銀行への登録に該当する。その時、認証のための証拠として後日用いるものを、合わせて登録しておく。いわゆる届け出印がその証拠であるが、ＡＴＭ機での預け入れ／引き出しの時に用いる暗証番号も届け出印と全く同じ効果を持つ。つまり、引き出しを行う際に間違いなく本人の口座から払い出すために、払い出しを請求する者が本人か否かの確認を行う必要があり、そのために、届け出印または暗証番号が使用される。

【０００４】（クレジットカードにおける認証）また、クレジットカードを利用して買い物をする場合には、買い手は商店に対して、自分はその商店が加盟しているカードシステムの会員であることの証拠として、各カード会員が所持するカードを提示する必要がある。そのカードシステムへの加入手続きが事前登録に該当する。この意味で、クレジットカードで用いられる認証は、カードという所有物による認証であるが、カードの盗難や遺失に対応するために、別途所有者認証を併用している。所有者認証には、例えばカード裏面の署名と書いての署名との照合が行なわれる。商店主は、カード伝票に署名される署名とカード裏面の署名とを比較して検証することで、買い手がカードの正しい持ち主であることを確認することができる。

【０００５】（アクセス管理における認証）コンピュータシステムへのアクセスにおいては、その利用者がアクセスしてもよい情報だけにアクセスを許すように、アクセス制御を行うのが普通である。アクセス制御は、誰がどのファイルへのアクセス許可を持っているかという登録に従った制御であり、利用者が誰であるかをシステム運用側が確認するのが必須の前提になっている。この確認は、ログイン時に提示されたパスワードとあらかじめ利用者登録時に登録されたパスワードとの比較照合で行われている。

【０００６】（入場時の認証）コンピュータシステムでなく、物理的な施設への入場／入室管理も全く同じ原理で行われる。入場が可能なのは、あらかじめ施設管理者に登録した人に限定される。入場時には、その人が登録されている個人であることの確認が行なわれる。確認には、身分証明書の目視確認、指紋認証システム、パスワードなどが用いられている。

【０００７】

【発明が解決しようとする課題】しかしながら、上記従来の認証システムにおいては、基本的に以下のような不具合があった。

【０００８】預金情報確認や口座引落し、インターネットなどの通信回線を用いた情報授受には、契約者個人で

6

あることの認証が必要となる。その認証の際には、あらかじめ個人が決めた認証番号・記号を、その都度、照合する形で検証するのが一般的である。このような認証は、極めて簡単に登録できる上、その照合についても簡便に行えるメリットがある。

【０００９】しかし、現在のようにあらゆるメディアのネットワーク化が進む中で、各種の認証番号・記号を設定する対象が増えていくと、各種の認証番号・記号を記憶に留めておくのが困難になってくる。そのため、認証番号・記号を、個人の覚えやすいある特定の番号・記号に統一したり、何かに記入して保管するといったことを余儀なくされてしまうが、これらの行為は、認証番号・記号の盗用の危険を高くしてしまうことになる。

【００１０】本発明の目的は、第三者の盗用のおそれを低減するための認証システム及び認証システムに用いられる認証請求装置，検証装置及びサービス媒体の提供を図ることにある。

【００１１】

【課題を解決するための手段】本発明の認証システムは、認証請求者からの請求に応じて、認証者が認証請求者の適格性を認証する際に用いられる認証システムであって、上記認証請求者に固有の認証請求用の固定情報と、時間的に変動する特性を有する変動情報とを受け、上記認証請求用の固定情報と上記変動情報とに基づいて、暗号情報を作成する暗号情報作成手段と、上記認証請求用の固定情報に対応する認証用の固定情報と、上記暗号情報とを受けて、上記暗号情報から少なくとも上記認証請求用の固定情報を復元する情報復元手段とを備えている。

【００１２】これにより、認証請求用の固定情報は認証システム内を流通するだけで、認証システム内に格納されている必要がないので、第三者が認証請求者固有の固定情報を検知することが困難となる。しかも、暗号情報には、認証請求者の位置，時間などに応じて変化する変動情報が含まれているので、第三者が固定情報を盗用することの困難性が増大する。よって、認証システムを利用する際の第三者の盗用のおそれを低減することができる。

【００１３】上記認証請求者に固有の認証請求用のもう１つの固定情報を記憶する第１の固定情報記憶手段と、上記認証請求用のもう１つの固定情報に対応する認証用のもう１つの固定情報を記憶するもう１つの固定情報記憶手段とをさらに備え、上記暗号作成手段は、上記認証請求用のもう１つの固定情報をも含めて上記暗号情報を作成し、上記情報復元手段は、上記認証請求用のもう１つの固定情報をも復元することにより、第三者の盗用のおそれがさらに低減される。

【００１４】上記情報復元手段及び上記もう１つの固定情報記憶手段の出力を受けて、上記認証請求用のもう１つの固定情報と上記認証用のもう１つの固定情報とを照

合する照合手段をさらに備えることにより、認証の確実性が向上する。

【００１５】上記復元手段は、上記変動情報をも復元し、上記復元された上記変動情報を受けて、変動情報に基づいて、認証請求者の適格性を判定する判定手段をさらに備えることにより、認証の確実性がさらに向上する。

【００１６】上記暗号情報作成手段は、暗号作成用の公開情報をも用いて上記暗号情報を作成し、上記情報復元手段は、暗号解読用の公開情報をも用いて上記復元を行なうことにより、暗号作成及び復元動作の円滑化を図ることができる。

【００１７】上記認証者が複数存在しており、上記認証請求用の固定情報は、各認証者に対して共通化されていることにより、第三者の盗用のおそれを低減しつつ、認証請求者が多数の暗号番号を使用するような煩雑さを回避することができる。

【００１８】上記暗号情報作成手段と上記情報復元手段とは、１つの媒体に組み込まれており、上記媒体は、音声信号及び映像信号のうち少なくともいずれか１つを生成するための回路と、上記復元された上記認証請求用の固定情報を受けて、上記固定情報に基づいて、上記回路の作動・非作動を制御する制御手段とをさらに備えていることにより、映像配信や音楽配信のサービスに適した認証システムを構築することができる。

【００１９】本発明のもう１つの認証システムは、認証請求者からの請求に応じて、認証者が認証請求者の適格性を認証する際に用いられる認証システムであって、少なくとも時間的に変動する特性を有する変動情報を受け、上記変動情報に基づいて、暗号情報を作成する暗号情報作成手段と、請求用の固定情報に対応する認証用の固定情報と、上記暗号情報とを受けて、上記暗号情報から少なくとも上記変動情報を復元する情報復元手段とを備えている。

【００２０】これにより、暗号情報には、認証請求者の位置，時間などに応じて変化する変動情報のみが含まれているので、第三者が認証請求者の情報を盗用することの困難性が増大する。よって、認証システムを利用する際の第三者の盗用のおそれを低減することができる。

【００２１】上記変動情報の適否判定のための登録情報を記憶する登録情報記憶手段と、上記登録情報に基づいて、上記復元された変動情報の適否を判定する適否判定手段とをさらに備えていることにより、認証を容易に行なうことができる。

【００２２】本発明の認証請求装置は、認証請求者からの請求に応じて、認証者が認証請求者の適格性を認証する際に用いられる認証システム中の認証請求装置であって、時間的に変動する特性を有する変動情報を受ける変動情報入力部と、上記変動情報入力部を受け、上記変動情報に基づいて、暗号情報を作成する暗号情報作成手段とを備えている。

【００２３】これにより、暗号情報には、認証請求者の位置，時間などに応じて変化する変動情報のみが含まれているので、第三者が認証請求者の情報を盗用することの困難性が増大する。よって、認証請求を行なう際の第三者の盗用のおそれを低減することができる。

【００２４】上記認証請求者に固有の認証請求用の固定情報を受ける固定情報入力部をさらに備え、上記暗号情報作成手段は、上記固定情報と上記変動情報とに基づいて、上記暗号情報を作成することが好ましい、その場合にも、認証請求用の固定情報は認証請求装置内を流通するだけで、認証請求装置内に格納されている必要がないので、第三者が認証請求者固有の固定情報を検知することが困難となる。

【００２５】上記認証請求者に固有の秘密性を必要とする認証請求用のもう１つの固定情報を記憶する第１の固定情報記憶手段と、上記認証請求用のもう１つの固定情報に対応する認証用のもう１つの固定情報を記憶する第２の固定情報記憶手段とをさらに備え、上記暗号作成手段は、上記認証請求用のもう１つの固定情報をも含めて上記暗号情報を作成することにより、第三者の盗用のおそれがさらに低減される。

【００２６】上記もう１つの固定情報は、認証請求者を識別する画像情報を基に作成されていることにより、第三者の固定情報の模倣が困難になる。

【００２７】上記変動情報は、ＧＰＳ（グローバル・ポジショニング・システム）に基づいて設定されているか、上記変動情報は、移動体情報端末および移動体基地局からの情報に基づいて設定されているかが好ましい。

【００２８】本発明の検証装置は、認証請求者からの請求に応じて、認証者が認証請求者の適格性を認証する際に用いられる認証システム中の検証装置であって、認証請求者から送られる，認証請求者固有の認証請求用の固定情報と変動情報とに基づいて作成された暗号情報を受ける暗号情報入力部と、上記認証請求用の固定情報に対応する認証用の固定情報を入力する固定情報入力部と、上記暗号情報作成入力部及び固定情報入力部の出力を受けて、上記暗号情報から少なくとも上記認証請求用の固定情報を復元する情報復元手段とを備えている。

【００２９】これにより、認証用の固定情報は検証装置内を流通するだけで、検証装置内に格納されている必要がないので、第三者が認証請求者固有の固定情報を検知することが困難となる。しかも、暗号情報には、認証請求者の位置，時間などに応じて変化する変動情報が含まれているので、第三者が固定情報を盗用することの困難性が増大する。よって、検証の際の第三者の盗用のおそれを低減することができる。

【００３０】上記認証請求者から送られる暗号情報には、認証請求用の固定情報に対応する認証用のもう１つの固定情報が含まれており、上記認証請求用のもう１つ

の固定情報に対応する認証用のもう１つの固定情報を記憶する固定情報記憶手段と、上記情報復元手段及び上記固定情報記憶手段の出力を受けて、上記認証請求用のもう１つの固定情報と上記認証用の固定情報とを照合する照合手段とをさらに備えることにより、検証の確実性が向上する。

【００３１】上記復元手段は、上記変動情報をも復元し、上記復元された上記変動情報を受けて、変動情報に基づいて、認証請求者の適格性を判定する判定手段をさらに備えることにより、検証の確実性がさらに向上する。

【００３２】本発明のもう１つの検証装置は、認証請求者からの請求に応じて、認証者が認証請求者の適格性を認証する際に用いられる認証システム中の検証装置であって、認証請求者から送られる変動情報とに基づいて作成された暗号情報を受ける暗号情報入力部と、上記暗号情報作成入力部の出力を受けて、上記暗号情報から少なくとも上記変動情報を復元する情報復元手段とを備えている。

【００３３】これにより、暗号情報には、認証請求者の位置，時間などに応じて変化する変動情報のみが含まれているので、第三者が固定情報を盗用することの困難性が増大する。よって、検証の際の第三者の盗用のおそれを低減することができる。

【００３４】上記変動情報の適否判定のための登録情報を記憶する登録情報記憶手段と、上記登録情報に基づいて、上記復元された変動情報の適否を判定する適否判定手段とをさらに備えていることにより、検証を容易に行なうことができる。

【００３５】本発明のサービス媒体は、認証請求者からの請求に応じて、認証者が認証請求者の適格性を認証する際に用いられる認証システム中の媒体であって、上記認証請求者に固有の認証請求用の固定情報を受ける固定情報入力部と、時間的に変動する特性を有する変動情報を受ける変動情報入力部と、上記認証請求用の固定情報と上記変動情報とを受け、上記認証請求用の固定情報と上記変動情報とに基づいて、暗号情報を作成する暗号情報作成手段と、上記認証請求用の固定情報に対応する認証用の固定情報と、上記暗号情報作成手段の出力とを受けて、上記暗号情報から少なくとも上記認証請求用の固定情報を復元する情報復元手段と、音声信号及び映像信号のうち少なくともいずれか１つを生成するための回路と、上記復元された上記認証請求用の固定情報を受けて、上記固定情報に基づいて、上記回路の作動・非作動を制御する制御手段とを備えている。

【００３６】これにより、認証用の固定情報はサービス媒体内を流通するだけで、サービス媒体内に格納されている必要がないので、第三者が認証請求者固有の固定情報を検知することが困難となる。しかも、暗号情報には、認証請求者の位置，時間などに応じて変化する変動

情報が含まれているので、第三者が固定情報を盗用して音楽信号や映像信号を利用することの困難性が増大する。よって、サービスを享受することについての第三者の盗用のおそれを低減することができる。

【００３７】本発明のもう１つのサービス媒体は、認証請求者からの請求に応じて、認証者が認証請求者の適格性を認証する際に用いられる認証システム中のサービス媒体であって、時間的に変動する特性を有する変動情報を受ける変動情報入力部と、上記変動情報に基づいて、暗号情報を作成する暗号情報作成手段と、上記暗号情報作成手段の出力を受けて、上記暗号情報から少なくとも上記変動情報を復元する情報復元手段と、音声信号及び映像信号のうち少なくともいずれか１つを生成するための回路と、上記復元された上記変動情報を受けて、上記変動情報に基づいて、上記回路の作動・非作動を制御する制御手段とを備えている。

【００３８】これにより、暗号情報には、認証請求者の位置，時間などに応じて変化する変動情報のみが含まれているので、第三者が固定情報を盗用して音楽信号や映像信号を利用することの困難性が増大する。よって、サービスを享受することについての第三者の盗用のおそれを低減することができる。

【００３９】

【発明の実施の形態】ー基本的な認証システムー

一般に、認証とは、認証請求者が、認証されるべき個人等であることをあらかじめ登録しておき、その証拠を示すことによって、当該個人等であること，つまり当人が適格性を有することを照合・確認する行為のことをいう。ここで、本発明における「認証請求者（被認証者）」には、個人だけでなく複数人，法人，団体，各種組織，グループなどが含まれるので、本明細書においては、これらを総称して「個人等」というものとする。また、ここで言う登録という行為は、何らかの目的を果たすために行われるものであり、個人等の認証もまた何らかの（登録の目的と通常同じ）目的を果たすために行われる。

【００４０】例えば、あるサービス（これはかなり広い意味でのサービスであるが）を享受したいが、そのサービスを享受しうる個人等が予め限定されている場合を想定する。このとき、個人等がサービスの提供を請求すると、当該個人等が確かにそのサービスを享受できる個人等であることを確認して始めてサービスを享受することができる。このような仕組みにおいて、認証が必要になり、この場合、上述の目的とはサービスを享受することである。

【００４１】１．認証の原理

前述したように、認証とは、認証請求者が、あらかじめ登録されている個人等であること，つまり認証請求者の適格性を確認する行為である。そのためには、登録した個人等であることを何等かの形で証明させるプロセスを

11

経る必要がある。この証明の方法には後で述べるような幾つかの方法があるが、まず、認証請求者に証明に必要な情報又は物を提示させる（提示情報）必要がある。また、登録の一環として、ここでいう証明のための情報（登録情報）も併せて登録しておく必要がある。そして、登録情報と提示情報との照合によって、認証請求者が、あらかじめ登録されている個人等であることを確認するのが一般的な認証の原理である。登録情報として物を用いる場合には、当該物が登録時に登録側から発行される必要があり、確認は確かに個人に交付された実物であることの確認を行うことになる。

【００４２】図１は、一般的な認証システムにおける認証の流れを模式的に示すブロック図である。

【００４３】同図に示すように、認証請求者１１が認証請求者の所有物１３から提示情報１４を示すと、認証者１２の依頼を受けて検証を行なう検証者又は検証システム（検証機関１６）から登録情報１７が示されるので、提示情報１４と登録情報１７とを照合することにより認証が行なわれる。

【００４４】ここで、図１に示す認証システムにおける各基本要素の定義は、

認証請求者：自分が登録してある個人等に間違いないことを主張する個人等

検証者：認証請求者の主張をその裏付けによって確認する人（またはシステム）

認証者：照合結果を最終的に判断して、認証請求者が当該個人等である事を確信する人

登録情報：認証の際の確認の裏付けとして登録し、検証者が利用する情報

提示情報：認証請求者が証拠として提示する情報（検証者により登録情報と比較検証される情報）

の通りである。

【００４５】２．認証の方式

認証を行うには、個人等であることを示す情報として何を用いるかによって以下に示す各種の方式に分類できる。

【００４６】Ａ．個人の場合ー

（バイオメトリクスＩ）特に、人体の生物学的特徴を表す部分を利用するもので、他人が意図的に変化させることができない部分を利用する。具体的に、生物学的特徴を表す部分としては、顔，指紋や網膜における血管パターン、虹彩の模様などがある。

【００４７】・顔

人の顔には個人差があり、顔自体の特徴を利用する認証技術は、一番古くから用いられてきた技術と考えられるが、コンピュータを利用する場合には、顔画像（写真）の照合を行なうことになる。ただし、登録情報としての顔画像と、認証時に撮影される提示情報としての顔画像とは、時期や場所などの撮影条件が異なるため、両者の照合に対しては、単なる顔画像同士の一致ではなく、さ

12

まざまな特徴点を抽出して、特徴点同士の一致により、確認を行なう必要がある。

【００４８】顔の特徴としては、顔の外形(輪郭)、眼の形、鼻の形、口の形、顔の起伏など用いる研究例が報告されている。顔による個人識別はアルゴリズムを含め、なお研究段階にあり、現時点では、民生に利用可能な製品は未発表である。

【００４９】・網膜

網膜中には外部から見える血管が存在しており、網膜上の血管パターンは各人各様であるために、網膜を個人の識別に使うことが可能であるといわれている。網膜中の血管パターンを見るには、専用器具に認証請求者の眼を近づけ、外部から光を当てる必要がある。網膜による認証技術はある程度確立した技術ということができ、米国のEyedentify社から製品が発売され、かなりの利用実績がある。ただし、網膜の観察には特殊な機器を必要とするので適用領域は入退室管理もしくはそれに類するところに限られているのが現状である。

【００５０】・虹彩

網膜と同様に、眼の一部である虹彩の模様も個人毎に異なるといわれている。網膜は眼の奥に位置していて、眼を専用器具に近づけて外部から光を当てないと網膜は見えないのに比べて、虹彩は、眼の表面に現れていて、特殊な専用器具を用いなくても容易に見ることができる。このため、虹彩の撮影は、通常のビデオカメラやデジタルカメラのような汎用的な撮像装置によって可能であり、認証システム中に導入しやすいとう利点がある。

【００５１】・耳

耳の形の個人差に関しては欧米でも日本でも研究報告がなされており、耳の形は万人不同であるといわれている。また、耳の大きさは、長さ，幅ともに１６～１７才以降は安定期に入り、その後若干の成長が見られるが、終生不変とみなすことができる。しかし、親子，兄弟，姉妹，双子間においても識別可能かどうか、つまり、遺伝的側面からの万人不同性の検証については、なお研究が必要といわれている。

【００５２】現在、耳の形が万人不同であることを前提として、耳の形の識別・同定実験が重ねられており、識別・同定のアルゴリズムも研究途上にある。こうしたことから、耳の形による認証については、可能性はあるものの未だfeasibilityも含めて研究段階であり、現段階では実用に至っていない。

【００５３】・指紋

指紋は万人不同といわれており、指紋を利用した認証技術は、個人を識別するバイオメトリクスとして、一番信頼感がある。指紋による個人同定の方法については、古くから法科学の分野で確立されていたが、以前はコンピュータによる処理方法だけが未確立であった。しかし、以前からコンピュータによる認証システムに指紋を利用するための研究が重ねられてきた結果、現在では、指紋

の利用は技術的にほぼ確立されたと考えてよい。この認証方式は、既に色々なメーカで製品化が行われ、実用化されている。方式的にはマニューシャマッチング方式と画像マッチング方式とに大別できるが、マニューシャマッチング方式による製品が多いようである。

【００５４】富士通、三菱、ＮＥＣ、ＳＯＮＹ、日商岩井、日本ＬＳＩカード、浜松ホトニクス、松村エレクトロニクス、山武ハネウェル、翼システム、セコムなどから製品が発表されている。

【００５５】・掌紋

掌紋を利用する認証技術は、手のひらのしわの形状の特徴を利用するものであるが、指紋ほどの特徴点が多くないため、個人識別の精度は指紋におよばない。また、一般に、掌紋は指紋ほどの万人不同性を有しているとは考えられていないので、現状では、認証のために掌紋を利用することができる分野は限定されざるを得ない。現在、掌紋を利用した認証方式については、開発中を含めて幾つかの製品がでており、入退室管理など比較的要求条件の緩いところでは使われるのではないかと考えられる。

【００５６】・掌形

掌紋が俗にいう手相の特徴を使うのに対して、掌形はいわゆる手形であって、掌形を利用する認証技術は、手のひらの幅や長さ、指の長さや形、などの特徴を捉えて利用するものである。掌形も、掌紋と同じく、指紋ほどの個人識別性があるとは考えられていないが、利用が簡単なので、やはり入退室管理などの限定された局面での利用が考えられる。現在、掌形を利用した認証方式については、国内外の数社で製品化されており、アトランタオリンピックで入退室管理に使われた実績がある。

【００５７】この方式のシステムについては、Recognition System、BioMet partners、Bio-metric Security Sys、三菱電機から製品が発表されている。

【００５８】・指形

指形を利用する認証技術は、指の関節で区切られた部分の長さが個人的なばらつきを持つ点に着目したものである。この方式と同様のアイデアとして、字の書けない人が署名代わりに指形を利用できる制度が、我が国で古くからあった。指形も、掌紋や掌形と同様に、指紋ほどの個人識別性が実証されていなくて、認証のために利用しうる範囲が限られると思われる。現在、東芝がこの技術を入退室管理システムとして組み込んで製品化しているだけである。

【００５９】（バイオメトリクスII（署名／筆跡、声紋など））このバイオメトリクスIIの方式は、広い意味での生物学的特徴を利用するものであるが、意図的に変化させることが可能な特徴を利用するもので、その特徴を利用して他人に成りすます可能性を秘めている。署名（筆跡）や声紋などが、バイオメトリクスIIに該当する。

【００６０】・声紋

発声という行為は随意的な要素があるため、必ずしも再現性があるとは言えない。したがって、声紋を利用した認証技術においては、登録時と認証時との差を小さくするような配慮が必要である。音声信号は音圧の時間変化のデータであるが、音圧を周波数成分に分解して得られる周波数スペクトラムの時間変化のデータが声紋グラフである。声紋同士の照合は、登録された声紋データと同じ言葉の声紋データを採取し、両者のマッチングを調べるものである。前述のように、声紋には必ずしも再現性はないので、両者の照合は、単純な声紋データ同士の重ねあわせではなく、話者の特徴を認識・抽出した上で、その特徴同士のマッチングを調べることで行なわれている。この方式においては、登録すべき語句によっても再現の度合いは異なり、普段発声し慣れた語句の方が再現性が高いといわれている。この理由で、個人の名前などを認証に用いた例がある。

【００６１】声紋を認証に利用した実用例としては、米国のスプリント社の公衆電話用クレジットカードシステム"Voice Phone Card"がある。これは、ＴＩ社の技術を用いて実現されたものでユーザはガイドメッセージに従って１０桁の社会保障番号を発声するやり方を採っている。日本では、最近富士通からテレホンバンキングという名前で発表されたシステムがある。音声の研究は音声認識を目的として長い歴史があるが、認証のための個人同定・識別に関しては、アルゴリズムを含めてなお研究段階である。

【００６２】・署名

署名を用いる認証技術は、筆者認識技術の内の筆者照合技術を利用したものである。ちなみに筆者認識には筆者識別と筆者照合とがある。筆者識別とは筆跡から筆者が特定の複数の人物のうちの誰であるかを特定する技術であり、筆者照合とは筆者が特定のある人物であることを確認する技術である。筆者照合は対象となる人物の筆跡（今の場合、署名）をあらかじめ登録しておき、問題の筆跡と登録された筆跡との類似度を判定するものである。

【００６３】筆跡の形だけを問題にする静的署名と、筆順、筆圧、運筆速度などをも問題にする動的署名とがあるが、当然ながら動的署名の方が利用できる情報が多い。この場合にはタブレット等の専用機器の上で書く必要がある。現在実用化されているものには動的署名を用いる方式が多い。実用製品の例としてCADIX社のCyber-signを挙げておく。

【００６４】ここで、あげたバイオメトリクスＩＩの特質として、バイオメトリクスＩＩは個人が意志で変化させることができない特徴であるのに対して、バイオメトリクスＩＩは、個人が意図的に変化させることができるものである。これは、指紋等は他人に似せることはできないが、筆跡、声は他人の特徴を模倣することができる

からである。

【００６５】従って、バイオメトリクスＩＩを用いた認証技術は、個人の署名や声を真似て作られた提示情報を排除する必要がある。この点においてバイオメトリクスＩＩの場合とは、試験の方法が大きく異なることに留意する必要がある。

【００６６】Ｂ．複数人，法人，団体，各種組織などの場合

複数人，法人，団体，各種組織などの場合には、１人の代表者のみが認証のための登録を行なっている場合、あるいは複数人の各人、法人，団体，各種組織，グループの各構成人それぞれが個別に認証のための登録を行なっている場合は、既に説明した個人の場合の認証方式がそのまま適用される。

【００６７】一方、法人，組織などとして認証のための登録を行なっている場合には、例えば社印や当該団体のマークなどの２次元的パターン、コード番号などを認証のための登録情報として用いることができる。この場合、バイオメトリクスIIと同様に、模倣をいかに防ぐかが重要となる。

【００６８】３．所有物

所有物認証は、コンピュータ以前から認証の手段として広く利用されてきた技術である。具体的には、パスポート、身分証明書、運転免許証、会員証、クレジットカード等を利用するシステムがある。所有物認証は、個人等であることを証明するものを発行し、それを所持する者を当該個人等と認める考え方に立つものであるが、純粋な所有物認証では、盗難や遺失によって他人が成りすますリスクを内在しており、それを軽減するために所有者認証を併用している場合が多い。パスポート、身分証明書、運転免許証における顔写真は所有者認証のための登録情報である。また、クレジットカードでは署名（Signature ）を用いた所有者認証が使われている。銀行のキャッシュカードも所有物認証に分類されるが、所有者認証には暗証番号が用いられている。

【００６９】また、コンピュータの世界では、パスワードや暗号鍵などを格納するために磁気カードやＩＣカードを利用するケースが良くあり、操作上からは所有者認証を伴わない純粋の所有物認証に該当するが、人の頭に記憶しきれない情報を格納するための補助記憶として上記のカードを使っているに過ぎず、認証技術の分類の観点からは秘密情報による認証に分類すべきものである。

【００７０】さらに、ネットワークを介しての認証では、純粋な所有物認証は意味を持たない。すなわち、ネットワーク上で相手に提示しうるのは、電子情報以外に有りえず、コピー自在の電子情報においては、純粋な所有物認証が原理的になり立たないのは明らかである。従ってネットワークを介した所有物認証は所有者認証を併用し、所有者認証をネットワークを介して行うことで、間接的にその所有物を持った人を特定する方式にならざるをえない。従って、この場合は所有者認証を行う方式によって分類されることになる。

【００７１】４．秘密情報１

秘密情報を利用する方法も所有物認証と並んで古来から使われてきた認証の手段である。コンピュータの世界ではパスワードや暗証番号・ＰＩＮ（Personal Identification Number）と呼ばれる方式である。パスワード等の秘密情報による認証は確立された技術と言ってよく、それ自体には今更調べるほどのものはない。登録情報から提示情報を生成できるものを秘密情報１と分類する。

【００７２】利用されるネットワークが従来のクローズ環境からオープン環境に移行するにつれて、単純なパスワード方式は盗聴＋replayの手法で簡単に成りすましが可能になることから、ネットワーク上を裸のパスワードを流さない方法が研究開発され、実用化されてきている。

【００７３】これらのなかで最初に考案されたのは、ワンタイムパスワード（One Time Password）と呼ばれる方式で、更に以下の方式がある。いずれも実用化されて製品が市販されている。

【００７４】・チャレンジレスポンス方式

認証側からチャレンジと呼ぶ乱数列を提示し、認証請求者はこの乱数列に一定の操作・変換を加えたもの（これをレスポンスと呼ぶ）を生成して送り返す。上記の一定の操作・変換は利用者毎に異なり、認証者側に登録されている。すなわちこの操作・変換手順が個人情報に他ならない。

【００７５】提示される乱数列は毎回異なるので、ネットワーク上を監視してこれらを盗聴してもreplayには利用できない。この操作・変換手順は複雑で記憶するには情報量が大きすぎ、毎回手動操作するには運用性が悪くなる問題があるので、電卓用のハンドヘルドデバイスにチャレンジをレスポンスに変換する機能を内蔵させる実現方法を採る事が多い。

【００７６】この方式自体は新しいものではなく、日本では昭和３０年代に試作されたＥＴＳＳで既に採用されている。

【００７７】この操作･変換手順として、暗号化機能を用いることもできる。この場合、登録情報は（アルゴリズムと）暗号鍵となる。

【００７８】・同期方式

チャレンジレスポンス方式と似たハンドヘルドデバイスを利用するが、チャレンジはなく、認証者側の内部クロックとハンドヘルドデバイスのクロックを同期させておき、時刻の関数として双方で生成された時限パスワードを利用するものである。つまり利用者はその時点でハンドヘルドデバイスに表示されるものをパスワード（提示情報）として入力し、認証者側ではその時の時刻と利用者のＩＤを元にしてパスワード（登録情報）を生成して照合確認する方式である。

17

【００７９】５．秘密情報２

秘密情報１に分類したものは、登録情報が知られるとそれを元に提示情報を作ることが可能であり、１対１ないし１対ｎの関係では安全であるが、ＥＣのようなｎ対ｎの関係においては必ずしも安全とはいえない。登録してある情報が漏れても、提示する情報につながらない方式を秘密情報２と分類する。

【００８０】本質的には上の秘密情報２と同じであるが、例えばデジタル署名を用いる方式では、登録してあるのは公開鍵であり、提示するのはそれに対応した秘密鍵で署名した情報であって、登録してある公開鍵を入手しても、提示する情報を作成できないので、ここでは区別して別のカテゴリーに分類しておく。零知識証明を用いるものもこれに属する。

【００８１】このほかにクライアント／サーバシステムにおいてサーバー毎にパスワードを持つ煩雑さと裸のパスワードがネットワーク上を流れる危険性とを解決する目的のもと、米国ＭＩＴで開発されたＫｅｒｂｅｒｏｓがある。個別の機能サーバとは別に認証サーバを設けて、クライアントはこの認証サーバから目的とする機能サーバへの電子的身許保証状（ticketと呼ぶ）をもらい、目的サーバにこれを提示する考え方をベースとしている。第三者認証方式とも分類される。

【００８２】このticketは共通鍵暗号による所有者認証を併用した一種の所有物認証とも考えることが出来る。なおticketには有効期限が設定される。これはＵＮＩＸ（登録商標）をベースとしたクライアント／サーバシステムで実用化されているが、現段階のＥＣ環境では主流にはなっていない。

【００８３】（第１の実施形態）上記のような背景に鑑み、本実施形態では、個人の暗証記号を設定するに際して、従来のようなあらかじめ決めておく個人情報（記憶、所有物も含む）だけではなく、そのときの個人がいる位置に関する情報および時間に関する情報を変動情報として採用し、これらの情報群を基に認証を行なう技術について説明する。すなわち、変動情報もを組み込んだ暗証番号を、特定の情報作成手段を用いてその都度作製し、認証の必要なときに、あらかじめ登録された個人情報の一部と認証情報を作成した際のデコード情報とを基にして、個人の認証情報を復元し、個人のリアルタイムの情報と共に認証を行い、その位置情報および時間情報の経過をたどることを可能とし、これにより、認証の精度を高め、個人暗証番号・記号の盗用をより高度に防ぐシステムについて説明する。

【００８４】ただし、本実施形態では、個人の認証を例にとって説明するが、法人，団体，各種組織についても、場所，時間などの情報を暗唱記号に組み込むことができるので、本発明を適用することができる。

【００８５】また、本実施形態においては、便宜上、位置情報も変化するものとして説明しているが、組織などの場合には位置が変動しないこともある。その場合でも、他人が異なる場所から組織のコード番号などを用いても、当該組織になりすますような事態を防止することができるので、本発明の変動情報は、必ずしも位置が変動しなくても、時間的に変化する情報であればよい。

18

【００８６】図２は、本発明の第１の実施形態の認証システム全体の構成及び情報の流れを概略的に示すブロック図である。

【００８７】認証請求者１１は、認証請求者に固有の第１の固定情報である認証請求用の暗号鍵４１を保有している。そして、認証者１１の所有物１３には、適当な暗号処理から決定されている個人に対応した公開鍵４２と、上述のバイオメトリクスなどを利用した，認証請求者に固有の第２の固定情報であるバイオメトリクス情報４４とが格納されている。ただし、所有物１３には、暗号鍵４１は格納されておらず、認証請求の際にその都度入力されるだけである。また、所有物１３は、３衛星を用いたＧＰＳシステムや携帯の基地局などの変動情報提供者４７から変動情報４５を受け取る機能を有している。さらに、所有物１３は、変動情報４５を用いて提示情報１４を作成する機能を有している。ただし、所有物１３が提示情報１４を作成する機能を有しておらず、提示情報を作成する機能を有する装置が別に存在していてもよい。

【００８８】また、この例では、認証者１２は検証部１６Ａを備えている。ただし、認証者１２とは別に、検証者，検証装置などを有する検証機関が存在していてもよい。認証者１２は、あらかじめ認証請求者１１との取り決めによって個人情報である認証用の暗号鍵４３を保有しており、この例では、認証者１２が検証部１６Ａを保有していることから、認証用の暗号鍵４３は検証部１６Ａに格納されている。また、検証部１６Ａには、認証請求者１１から提供されたバイオメトリクス情報４４などの登録情報１７が格納されている。ただし、暗号鍵４３は必ずしも検証部１６Ａ内に格納されている必要はなく、認証者から認証時に入力されるようにしてもよい。

【００８９】すなわち、認証請求者１１は、所有物１３と切り離して記憶する第１の固定情報を認証請求用の暗号鍵４１として用意し、認証者１２はこの暗号鍵４１から、その都度用意される暗号様式に従って、認証者固有の認証用の暗号鍵４３および両者固有の共通鍵である公開鍵４２を設定する。認証請求者１１の設定した公開鍵４２を、認証者１２あるいは検証部１６Ａに登録しておくことが好ましい。また、運用を簡便にする上で、この例のごとく所有物１３にはを登録しておくことが好ましい。ここでの所有物１３は、前述した機能を有するものであれば、必ずしも専用器ある必要はなく、バイオメトリクス情報４４などの第２の固定情報を付加することで、個性を発揮するものであればよい。さらに、認証者１２は、検証部１６Ａにバイオメトリクス情報４４など

の第２の固定情報を登録させることが好ましい。

【００９０】認証請求者１１は、その所有物１３を用いて認証を請求するが、その都度暗証番号を作成する必要がある。そこで、所有物１３に認証請求用の暗号鍵４１が入力されると、認証請求用の暗号鍵４１と公開鍵４２（暗号作成用の公開情報）とが合わせられることにより、あらかじめ所有物に登録されたバイオメトリクス情報４４と、変動する位置，時間などに関する変動情報４５とから暗号情報４６が算出される。

【００９１】次に、算出された暗号情報４６と公開鍵４２とは、提示情報１４として検証部１６Ａに送られる。あるいは、提示情報１４は、認証者１２に提示された後、認証者１２から検証部１６Ａに送られてもよい。

【００９２】検証部１６Ａでは、提示された公開鍵４２（暗号解読用の公開情報）を手がかりに認証用の暗号鍵４３が選択され、認証用の暗号鍵４３と公開鍵４２とを用いて暗号情報４６がデコードされる。そして、デコードされた情報の中のバイオメトリクス情報４４ａと、あらかじめ登録情報１７中に格納されているバイオメトリクス情報４４ｂとの照合が行われる。そして、各バイオメトリクス情報４４ａ，４４ｂの一致・不一致が判定されて個人の認証が完了することになる。また、復元された位置，時間などに関する変動情報４５ａと、検証部１６Ａで時間などに基づいて演算された変動情報４５ｂとの一致・不一致を判定する。また、復元された位置，時間などに関する変動情報４５ａは一定期間保存され、個人の軌跡情報として用いられる。ただし、変動情報４５ａを認証のために用いなくてもよい。

【００９３】本実施形態の認証方法によると、以下の作用効果が得られる。認証請求者１１が認証を求める場合、まず、所有物１３に認証請求用の情報を入力する必要がある。従来技術では、第１の固定情報である暗号鍵４１に相応する情報（又は、第１の固定情報である暗号鍵４１と第２の固定情報であるバイオメトリクス情報４４）を直接検証に用いていたので、所有物１３にデフォルト値として残ることになる。それに対し、本実施形態によれば、第１の固定情報を認証請求時の揮発情報である暗号鍵４１としてのしか用いないため、所有物１３には第１の固定情報がデフォルト値として残らない。よって、第１の固定情報を第三者に盗用されるおそれが極めて少ない。

【００９４】なお、第２の固定情報であるバイオメトリクス情報４４は必ずしも用いる必要がないが、これを用いることにより、第三者のシステムの悪用をより確実に防止することができる。

【００９５】また、本実施形態では、所有物１３は、認証請求の際の位置，時間などに関する変動情報４５を検出し、所有物１３に記憶されている第２の固定情報であるバイオメトリクス情報４４にそれらを併せて、第１の固定情報である暗号鍵４１と公開鍵４２とを用いて、変

動情報４５とバイオメトリクス情報４４とから暗号情報４６を作成する。そして、作成された暗号情報４６に公開鍵４２が付加されて、提示情報１４として、検証部１６Ａに送られる。このように、本実施形態では、提示情報１４中の暗号情報４６は、バイオメトリクス情報４４に変動情報４５が付加されているので、認証請求の際の信号から第三者が提示情報１４を検知したとしても、提示情報１４からバイオメトリクス情報４４を抽出することも困難である。よって、本実施形態により、第三者が認証請求者１１になりすまして認証に成功するおそれを抑制することができる。

【００９６】また、本実施形態では、検証部１６Ａは、公開鍵４２を用いて認証者１２から認証請求者固有の認証用の暗号鍵４３を選び出し、この２つの鍵を用いて、バイオメトリクス情報４４ａおよび変動情報である位置，時間などに関する変動情報４５ａを復元し、バイオメトリクス情報４４ａ，４４ｂ同士の照合と、位置，時間などに関する変動情報４５ａ，４５ｂ同士の照合とを行なっている。暗号鍵４３は、認証請求用の暗号鍵４１そのものではないので、従来技術に比べると、第三者の悪用防止の確実性がより高まる。

【００９７】また、変動情報４５ａ，４５ｂを一定時間蓄積してこくこともでき、その場合には、変動情報４５ａ，４５ｂを認証請求者１１の行動軌跡情報として、例えば認証請求者１１が認証請求時に特定の場所にいたことを証明する、などに利用することができるという利点がある。

【００９８】なお、認証完了後も長時間、暗号情報４６が検証部１６Ａを通過している場合には、上述の認証動作を定期的あるいは不定期に行なうのが好ましい。この際には、特に、認証には、バイオメトリクス情報４４ａ，４４ｂおよび個人の行動軌跡情報である変動情報４５ａ，４５ｂを用いるのが好ましい。

【００９９】また、ここでは、位置，時間などに関する変動情報検出のタイミングを認証請求者が計ったが、認証者によってそのタイミングを指定される場合もあり得る。仮に両者の情報授受を第３者が傍受しても、暗証記号に位置，時間などに関する変動情報が加わっている点で、第３者が別時間、別場所において認証システムにアクセスを試みても認証が許されることは極めて困難である。

【０１００】また、第３者が所有物の使用を試みた場合においては、所有物と切り離されている暗号鍵４１である第１の固定情報を有しないため、やはり認証が許されないのは現行通りである。

【０１０１】本実施形態で提案した暗証記号を構成する
１．第１の固定情報（暗号鍵４１）（所有物と切り離されて所有）
２．第２の固定情報（バイオメトリクス情報４４）（所有物に組み込まれて所有可）

３．変動情報（位置，時間などに関する変動情報）
４．暗号情報
は、目的に応じてその組み合わせを変えることが、システムの簡便な運用にとって好ましい。

【０１０２】第１のケースは、本実施形態のように、暗号情報として、第２の固定情報つまりバイオメトリクス情報４４と変動情報４５とが組み込まれたものを用いる場合である。この場合、第１の固定情報である暗号鍵４１，公開鍵４２は、いずれも必ずしも用いる必要がないが、本実施形態のように、これらの２つを用いた方がより確実性が高まる。

【０１０３】第２のケースは、暗号情報として、第１の固定情報情報である暗号鍵４１と、変動情報４５とを組み込んだものを作成して、暗号鍵４１と変動情報４５とを復元する方法である。その場合、復元された暗号鍵４１と検証部１６Ａに取り込まれた暗号鍵４３とを照合することができる。暗号鍵４３は容易に暗号鍵４１に変換することができるからである。その場合、バイオメトリクス情報４４と変動情報４５とを暗号情報に組み込んだものと基本的は似ているが、バイオメトリクス情報４４ｂは必ず検証部１６Ａに記憶されているのに対し、暗号鍵４１は後述する第３の実施形態のごとく、検証部１６Ａに記憶されていなくてもよいという点が異なる。

【０１０４】第３のケースは、暗号情報として、変動情報４５のみが組み込まれたものを利用する方法である。その場合、検証部１６Ａに記憶されている認証用の変動情報４５ｂは、あらかじめ認証請求者１１によって登録された登録情報であることが好ましい。例えば、あらかじめ利用する時刻が２時から３時の間と設定されていれば、変動情報４５中の時刻と設定時間とを照合することにより、これ以外の時刻に認証請求があっても拒否される。また、認証請求場所をある特定の範囲（市，都道府県など）に設定しておけば、変動情報４５中の場所と設定地域とを照合すれば、それ以外の地域からの認証請求は拒否されることになる。認証請求者が体重や体温など自己の特徴点で時間的に変動する性質のものを変動情報としておけば、第三者がこれを検知するのは困難であるために、第三者の盗用を抑制しうる効果が顕著になる。

【０１０５】また、認証請求者が第三者に問いかけを行なって、第三者からの返答を変動情報として用いることもできる。その場合、第三者は認証者であってもよいし、全く別の機関であってもよい。例えば、常時時刻を告知している電話システムを利用して、問いかけに対して返答された時刻を変動情報として利用することなどが可能である。

【０１０６】図２に示す認証システムにおいては、認証請求者１１は、認証者１２に対しての認証登録の契約に際して、本システムの使用を了承し、認証者１２あるいは検証者に対して、本システムの使用に対しての使用許諾を必要とする。使用許諾に対する課金については、本

システムに必要な認証信号検証用の端末およびサーバーの販売に際して執り行なうことができる。また、本システムを用いたサービスに対して課金を行なうことができる。

【０１０７】本システムによって運用可能なサービスとは、銀行ＡＴＭシステムサービスなどの金融機関との預け入れ／引き出しサービス、即時支払い型のキャッシュレスサービス、プリペイドあるいはクレジットサービス、インターネットなどを介した情報配信サービス、暗号化されて所有物に記録された行動軌跡情報を復元あるいは回収し個人情報として提供するサービスなどが挙げられる。特に、有線・無線に関わらず、ネットワークによる情報の配信に関するサービスについては、情報の配信経路と認証に関する経路を分離することにより、高密度の情報配信についても安全かつ効率的に情報授受者の認証を行うことができる。

【０１０８】さらに、ここで挙げた行動軌跡情報である変動情報４５の復元サービスは、携帯端末の所有者である認証請求者１１が暗号鍵４１を、第三者に提供することで所有物１３例えば携帯端末の所有権を一時放棄し、所有物１３中に記録された個人行動軌跡情報である変動情報４５を復元することで、個人のアリバイ証明としての情報を提供するものである。ただし、検証部１６Ａ中に記憶されている変動情報４５ａ（行動軌跡情報）を復元してもよい。その場合、復元サービスは認証者が行なうようにしてもよい。

【０１０９】（第２の実施形態）図３は、上記図２に示す認証システムに組み込むことが可能な本発明の第２の実施形態の認証請求装置の構成を概略的に示すブロック図である。ここでは、所有物１３の例である携帯端末１３Ａの構成を例にとって説明する。図４は、携帯端末中の変動情報検出部の構成を示すブロック図である。

【０１１０】図３，図４に示す各要素は、以下のような機能，構成を有している。個人情報を入力するための情報入力部３１は、コネクタ、キーボード、パネルスイッチ、イメージセンサ等の機能を併せ備えるデバイスによって構成されている。固定情報記憶部３２は、あらかじめ登録された個人情報を記憶するメモリデバイスによって構成されており、認証されるべき個人の特質を反映させた情報を記憶している。変動情報検出部３３は、位置，時間などに関する変動情報を検出する機能を有しており、例えば、図４に示す外部信号の受信アンテナ３７と、フィルタ，増幅器，ミキサー，Ａ／Ｄ変換器等を含み受信信号を復調するための復調部３８と、復調信号からのＣ／Ａコードから位置，時間などに関する変動情報を抽出するための変動情報抽出部３９と、位置，時間などに関する変動情報をいったん記憶して、行動軌跡を算出するための演算部４０とを備えている。認証情報演算部３４は、個人情報，変動情報を基に、認証情報を作成する機能を有している。情報記録部３６は、関連する情

報の記録部であり、ここには、演算部で作成された認証（暗号情報４６）や公開鍵４２が記録されている。入出力部３５は、認証情報を外部に出力する機能と、外部信号を入力する機能とを有している。信号の入出力には、接触型のコネクタあるいは非接触型のリーダを経由した入出力だけでなく、電波（高周波信号）・光による信号入出力を可能にするものであり、利用の形態に応じて、外部からの入出力デバイスは選定されるものとする。

【０１１１】なお、変動情報検出部３３は、ＤＣ（ダイレクトコンバージョン）式などのワンチップ器で置き換え可能に構成すれば、さらに有用性が向上する。

【０１１２】また、ここで所有物の一例として挙げた携帯端末１３Ａは、全体が物理的に一体である必要はなく、例えばその一部が装身器具としての機能を果たすように分割されていても、他の部分と共に上述の機能を果たしていればよい。例えば、受信アンテナを、パッチ型やリング型にして、装身具と共用することが可能である。実際、本発明の目的に応じて、位置，時間などに関する変動情報を検出する場合、ＧＰＳシステムを支える少なくとも３衛星を用いての位置特定を行なう必要はなく、装身具型のデバイスを用いてより少ない数の衛星からの情報による位置特定を行なってもよい。個人の行動範囲は、このような装身具型のデバイスを用いても、ある程度検出できることがわかっているからである。また、ＧＰＳシステムでなく、移動体情報端末および移動体基地局から送られる情報を利用しても、同等の位置，時間などに関する変動情報の検出を行なうことができることもわかっている。

【０１１３】固定情報記憶部３２に記憶される個人の情報としては、従来、金融機関で用いられているような個人の設定する単純な数桁の記号（数字を含む）、あるいは、先にバイオメトリクスＩ，ＩＩとして紹介した個人の顔や図形、文字等の画像や音声などの特定情報を用いることができる。バイオメトリクス的な情報は、所有物にあらかじめ記憶させておくことによっても運用が簡便になるため好ましい。

【０１１４】認証に際しては、あらかじめ登録されている個人情報を、認証を司る装置の端末に直接入力するか、携帯端末などの個人所有物を用いて間接的に入力することが可能に構成されていることが好ましい。また、それに加えて、ＣＣＤカメラあるいは感圧センサ等のイメージセンサによって個人情報を入力し、特定の情報作成手段を用いて番号・記号化されたものを、認証に用いるのもさらに好ましい。

【０１１５】変動情報検出部３３における位置，時間などに関する変動情報の検出に際しては、変動情報提供部４７から、基準となる電波信号や光信号を受信し、この信号に基づいて位置，時間などを算出する機能が重要である。屋外で変動情報を検出する場合は、通信衛星からの電波を受信して、受信者の位置を検出するＧＰＳを利

用することが好ましい。また、屋外で変動情報を検出する場合でも、携帯電話・ページャーなどの携帯端末に送られてくるローミング情報を用いても、位置，時間などに関する変動情報の入手が可能である。屋内で変動情報を検出する場合は、個人の体温を検知する赤外線センサー，体重検知センサー，個人の有する特定の端末などから発信される電波・光を用いて変動情報を取り込むことができ、どの手段を用いるかは設備の実施形態に合わせて選択することができる。これらの位置，時間などに関する変動情報は、ある特定の一時点を情報として利用するのみでなく、一定期間の軌跡情報も含めることが好ましい。一定期間の軌跡情報を用いることによって、さらに認証度が向上するからである。

【０１１６】整理すると、ここで挙げた認証に用いられる情報は、

１．第１の固定情報（所有物と切り離されて所有）
２．第２の固定情報（所有物に組み込まれて所有可）
３．変動情報（位置，時間などに関する変動情報）
４．暗号情報（携帯端末などで認証請求時に作成）

の大きく４種類の情報で構成される。

【０１１７】これらの１．２．３．４．の情報の組み合わせのバリエーションは、第１の実施形態で説明したとおりである。

【０１１８】ただし、公開鍵４２は必ずしも必要ではない。また、第２の固定情報であるバイオメトリクス情報４４は必ずしも用いる必要がないが、これを用いることにより、第三者のシステムの悪用をより確実に防止することができる。

【０１１９】本発明で提案される暗証記号によれば、従来の金融機関など多くの１．第１の固定情報のみによる照合に対してのリスクを低減し、３．変動情報のリアルタイムの位置，時間などの変動情報により、個人の行動軌跡が確認されるため、認証度の高いワンタイムパスワードを実現できる。

【０１２０】認証請求者１１は、上記第１の固定情報のうち少なくとも一部を所有物と切り離して持っていればよく、多様な個人暗証記号を有することができる。

【０１２１】上記認証情報演算部３４は、採取・選択された情報を、種々の認証情報作成手段を用いて番号・記号化する機能を有している。ここで用いられる作製手段の例としては、対称型の暗号作成法はもちろん、非対称型のＤＥＳ（Data Encryption Standard）に代表される共通鍵暗号作成、Diffie-Hellman法、ＲＳＡ法、Merkle-Hellman法などの公開鍵暗号作成、あるいは画像情報に対して電子透かし技術などを用いることが挙げられるが、これらに限定されるものではなく、目的に対して、より適切な暗号様式が随時組み込まれることが好ましい。

【０１２２】本発明でいう公開情報とは、共通鍵，公開鍵，電子すかし技術を用いる際の変換用媒体などを含む

25

が、これらに限定されるものではなく、暗号化するための情報と、暗号を解読するための情報であればよい。

【０１２３】このようにして作製される個人暗証番号・記号を用いた照合は、例えば以下の手順で行なわれる。まず、上記各種情報が記録された携帯型あるいは装身型の装置を用いて、個人が記憶するに耐える、あらかじめ登録した第１の固定情報である暗証番号・記号（暗号鍵４１）を認証請求装置１３Ａの情報入力部３１に入力する。この時、認証演算部３４内に組み込まれた認証情報作成手段を用いて、固定情報記憶部３２中のバイオメトリクス情報４４と、変動情報検出部３３から取り込まれた変動情報４５とから、番号・記号などからなる暗号情報４６が作製される。その後、認証請求装置１３Ａは、入出力部３５を介して、認証を司る装置の端末に接続された検証部に情報を伝送する。検証部では、上述のように、あらかじめ登録された認証用の情報の一部と暗号情報４６を作成した際のデコード情報（公開鍵）とを基にして、個人の暗号情報４６の復元を行なうことができる。

【０１２４】バイオメトリクス情報４４に付加された位置，時間などに関する変動情報４５は、認証用の情報である暗号情報４６の番号・記号の複雑化を可能にするだけでなく、暗号情報を構成する番号・記号の偽造・複製を防ぐのに効果的である。

【０１２５】なお、認証請求装置１３Ａを認証を司る装置の端末に接続し、センタへ情報を伝送する際に、接続した個人等に対して、簡単な質問を与え、その答えを暗号情報４６の作成に盛り込むことも、情報の複雑化にとって好ましい。

【０１２６】（第３の実施形態）図５は、本発明の第３の実施形態における検証装置１６Ｂの構成例を示すブロック図である。同図に示すように、本実施形態の検証装置１６Ｂは、暗号情報４６を含む提示情報１４などの外部信号を取り込んだり、外部に信号を出力するための入出力部５５と、公開鍵４２を格納している第１情報記憶部５６と、入出力部５５から取り込まれた提示情報４６から個人情報や変動情報を復元して認証情報を作成するための認証情報演算部５４と、暗号情報４６から復元された変動情報４５ａやバイオメトリクス情報４４ａを記憶するための第２情報記憶部５７と、復元された変動情報４５ａを検証のために演算するための検証演算部５９と、検証された変動情報を行動軌跡情報６０として記憶するとともに、あらかじめバイオメトリクス情報４４ｂを記憶するための第３情報記憶部５８とを備えている。

【０１２７】認証を行なう前の準備として、認証請求者は、所有物と切り離して記憶する第１の固定情報を認証請求用の暗号鍵４１として用意し、認証者１２はこの暗号鍵４１から、その都度用意される暗号様式に従って認証者固有の認証用の暗号鍵４３を設定する。また、認証請求者の設定した共通鍵である公開鍵４２，バイオメトリクス情報４４ｂは、あらかじめ検証装置１６Ｂの第１情報記憶部５６，第３情報記憶部５８にそれぞれ記憶されている。この公開鍵４２やバイオメトリクス情報４４ｂの格納は認証請求者がその所有物（携帯端末など）を通じて行なってもよいし、認証者１２が行なってもよい。

26

【０１２８】そして、認証請求者から、図２に示すようなバイオメトリクスなどを利用したバイオメトリクス情報４４と、位置，時間に関する変動情報４５とが合わさった暗号情報４６が作成され、暗号情報４６と公開鍵４２とを含む提示情報４６が、検証装置１６Ｂの入出力部５５に入力される。同時に、認証請求者から認証者１２に認証請求信号が伝達されるので、認証請求者１２は、この認証請求信号を受けて、検証装置１６Ｂ内の第１情報記憶部５６に認証請求の際に作成された暗号鍵４３を揮発性情報としていったん格納する。

【０１２９】すると、検証装置１６Ｂ内の認証情報演算手段５４は、第１情報記憶部５６に記憶されていた公開鍵４２と第１情報記憶部５６に取り込まれた揮発性情報である暗号鍵４３とを受けて、暗号情報４６から位置，時間などに関する変動情報４５ａと、バイオメトリクスなどを利用したバイオメトリクス情報４４ａとを復元して、これらの情報を第２情報記憶部５７に格納する。この復元の動作は、一般には、図３に示す認証請求装置１３Ａ中の認証情報演算部が行なう演算の逆演算である。

【０１３０】また、検証演算部５９は、第２情報記憶部５７から、復元された位置，時間などに関する変動情報４５ａを取り出して、変動情報４５ａがＯＫか否かの検証を行なう。ここでの検証の方法としては、各種の方法を採りうる。例えば、変動情報４５として時間，位置が組み込まれている場合、認証請求者の現在の位置を確認して、変動情報４５の内容である時間，位置と、認証請求者が検証の際に存在している位置とが矛盾していなければ、変動情報４５ａはＯＫであることを検証することができる。また、変動情報として体重計の信号が組み込まれた場合には、あらかじめ認証請求者が登録している体重と矛盾しなければ、変動情報４５ａはＯＫであることを検証することができる。

【０１３１】本実施形態では、暗号情報４６には暗号鍵４１を組み込まないが、暗号情報４６に暗号鍵４１を組み込んでもよい。その場合、暗号鍵４１，バイオメトリクス情報４４及び変動情報４５の組み込み方のバリエーションについては、第１の実施形態で説明した通りである。

【０１３２】そして、検証演算部５９は、変動情報の検証の結果、復元された変動情報４５ａがＯＫであった場合には、復元された変動情報４５ａを第３情報記憶部５８に行動軌跡情報６０として格納する。

【０１３３】また、照合部１５は、第２情報記憶部５７から復元されたバイオメトリクス情報４４ａを取り出

し、第３記憶部５８からあらかじめ登録されているバイオメトリクス情報４４ｂを取り出して、両者を照合し、バイオメトリクス情報４４ａ，４４ｂ同士が一致するか否かを判定する。この判定の手法としては、従来技術を利用して行なうことができる。

【０１３４】その結果、照合部１５や検証演算部５９から照合確認情報が外部に出力され、認証者は照合確認情報を受けて、認証請求者に認証の可・不可の返答を行なうことになる。

【０１３５】本実施形態の検証装置によると、以下の作用効果を発揮することができる。

【０１３６】まず、検証装置１６Ｂは、公開鍵４２と暗号鍵４３とを用いて、バイオメトリクス情報４４ａおよび変動情報である位置，時間などに関する変動情報４５ａを復元している。ここで、暗号鍵４３は、認証請求用の暗号鍵４１そのものではないので、従来技術に比べると、第三者の悪用防止の確実性がより高まる。しかも、本実施形態では、第１の実施形態のごとく暗号鍵４３が検証装置内にあらかじめ格納されているのではなく、暗号鍵４３は認証者から認証請求があったときのみ検証装置１６Ｂに揮発性情報として入力されるので、第三者が検証装置１６Ｂから暗号鍵４３を検知するおそれを第１の実施形態よりも確実に防止することができる。

【０１３７】仮に、両者の情報授受を第３者が傍受しても、暗号情報４６に位置，時間などに関する変動情報が加わっているので、第三者が別時間，別場所において検証装置１６Ｂにアクセスを試みても認証が許されることは極めて困難である。

【０１３８】また、認証を、バイオメトリクス情報４４ａ，４４ｂ同士の一致・不一致だけでなく、変動情報４５ａが合理的なものか否かをも考慮して行なっているので、認証の精度がより高くなる。

【０１３９】ただし、この演算検証部５９は必ずしもなくてもよい。バイオメトリクス情報４４ａ，４４ｂ同士の一致・不一致だけでも認証は可能だからである。また、バイオメトリクス情報４４ａ，４４ｂ同士が一致したときのみ変動情報４５ａの可・不可を判定するようにすることで、認証の精度を損ねることなく、認証に要する手間をより簡略化することができる。

【０１４０】なお、第２の固定情報であるバイオメトリクス情報４４は必ずしも用いる必要がないが、これを用いることにより、第三者のシステムの悪用をより確実に防止することができる。

【０１４１】また、行動軌跡情報６０を必ずしも保存しておく必要はない。ただし、本実施形態のごとく、行動軌跡情報６０を保存しておくことにより、個人のアリバイ証明としての情報を提供するなど、認証情報の利用性が高まる。

【０１４２】（第４の実施形態）図６は、本発明の第４の実施形態における認証システムの構成を概略的に示すブロック図である。同図に示すように、認証請求者１１に対してサービスを提供するための複数の認証者１２Ａ，１２Ｂ，１２Ｃが存在している。そして、認証請求者１１は、各認証者１２Ａ，１２Ｂ，１２Ｃから個別に提供された所有物１３Ａ，１３Ｂ，１３Ｃに暗号鍵４１を入力し、変動情報提供者４７から送られる変動情報４５と暗号鍵（４３ａ，４３ｂ，４３ｃ）とを合わせた暗号情報４６ａ，４６ｂ，４６ｃと公開鍵４２ａ，４２ｂ，４２ｃとを提示情報１４ａ，１４ｂ，１４ｃとして作成、各認証者１２Ａ，１２Ｂ，１２Ｃに入力する。そして、各認証者１２Ａ，１２Ｂ，１２Ｃの各検証機関１６は、提示情報１４に基づいて認証を行なう。このときの、各認証者１２Ａ，１２Ｂ，１２Ｃに対する認証請求者１１の所有物１３中における動作は、バイオメトリクス情報４４が含まれていない点を除くと、第１の実施形態において説明したとおりである。ここで、所有物１３Ａ，１３Ｂ，１３Ｃは、必ずしも物理的に別々の携帯端末などである必要はない。例えば、１つの携帯端末中に、各所有物１３Ａ，１３Ｂ，１３Ｃが組み込まれていても、上述の認証を個別の認証者１２Ａ，１２Ｂ，１２Ｃに行なうことが可能に構成されていればよい。

【０１４３】本実施形態では、暗号情報４６には暗号鍵４１を組み込まないが、暗号情報４６に暗号鍵４１を組み込んでもよい。その場合、暗号鍵４１，バイオメトリクス情報４４及び変動情報４５の組み込み方のバリエーションについては、第１の実施形態で説明した通りである。

【０１４４】本実施形態においては、多様なサービスを受ける場合に、従来のように各認証者ごとに、定められた単一の個人情報と単一の所有物と単一の暗号作成手段によって運用されるシステムとは異なり、多数の認証者に対して共通に設定された１つの暗号鍵４１を用いることができるという利点がある。

【０１４５】すなわち、本システムにおいても、認証請求者１１は第１の固定情報である暗号鍵４１のみを記憶するだけで、認証をもとめられる点では、従来例と形式的な違いはない。しかし、本システムにおいては、第１の固定情報である暗号鍵４１がそのままの形でシステム上を流れることはないので、認証に関する安全性は、従来に比べて大きく向上させることができる。

【０１４６】なお、本実施形態においても、第１の実施形態と同様に、認証請求者１１が、各認証者１３Ａ，１３Ｂ，１３Ｃに対して、自己の所有物１３に暗号鍵４１を入力し、図２に示すバイオメトリクス情報４４などの第２の固定情報と、変動情報提供者４７から送られる変動情報４５とを合わせた暗号情報４６ａ，４６ｂ，４６ｃと公開鍵４２ａ，４２ｂ，４２ｃとを提示情報１４として作成することもできる。その場合、各認証者１２Ａ，１２Ｂ，１２Ｃに対する認証請求者１１の所有物１３中における動作は、第１の実施形態において説明した

とおりである。また、このときの、各認証者１２Ａ，１２Ｂ，１２Ｃの各検証機関１２中における動作も、第１の実施形態において説明したとおりである。

【０１４７】また、第２の固定情報であるバイオメトリクス情報４４を用いるか否かは、サービスの認証レベルの高低において、その都度設定することもできる。

【０１４８】本実施形態では、認証請求者１１の所有物１３Ａ，１３Ｂ，１３Ｃは、サービス提供会社からそれぞれ個別に提供されるものとしたが、認証請求者１１の所有物１３自体は単一であるが、その中のメモリーにそれぞれのサービスに応じたプログラムを記憶するようにしてもよい。

【０１４９】以上のようなサービスを支える本実施形態のシステムは、サービスを提供する側とサービスを受ける側との両者に対して安全を与えるものであり、上記安全の保証度に応じて、本システムの安全不備に関する賠償責任を負う、いわゆる保険サービスを行なうことをも可能であるという特徴を有する。

【０１５０】（第５の実施形態）図７は、本発明の第５の実施形態における認証システムの構成を概略的に示すブロック図である。本実施形態は、上記第１～第４の実施形態における信号の流れを少し変えることにより、映像あるいは音楽などを情報として配信する情報配信サービスに関しても著作権を十分に守ることが可能な認証システムに関する。

【０１５１】本実施形態の認証システムは、情報配信者（図示せず）から情報受信者６１が、サービス媒体である所有物６３を購入するような仕組みとなっている。そして、認証者である情報配信者からの情報は、あらかじめ第１の固定情報である暗号鍵４３と、公開鍵４２とによって暗号化された暗号情報６６として、サービス媒体である所有物６３に付加されて販売される。すなわち、この所有物６３は、暗号情報６６と、情報配信者によって取り決められた公開鍵４２とが格納された状態で販売される。このとき、暗号情報６６は、所有物６３に付加された通信機能により、変動情報提供者４７から送られる時間，位置などに関する変動情報４５を取り込んで作成される。

【０１５２】ただし、公開鍵４２は必ずしも必要でない。また、第２の固定情報であるバイオメトリクス情報４４は必ずしも用いる必要がないが、これを用いることにより、第三者のサービス媒体の悪用をより確実に防止することができる。

【０１５３】本実施形態では、暗号情報４６には暗号鍵４１を組み込まないが、暗号情報４６に暗号鍵４１を組み込んでもよい。その場合、暗号鍵４１，バイオメトリクス情報４４及び変動情報４５の組み込み方のバリエーションについては、第１の実施形態で説明した通りである。

【０１５４】本実施形態においては、提供された暗号情報６６から配信情報を復元する場合、情報受信者６１は、別途、暗号鍵４３を手に入れ、それをサービス媒体である所有物６３に入力することで、情報復元作業を行なうことができる。演算部６７は、入力された暗号鍵４３と、あらかじめ所有物６３に付与された公開鍵４２とを用いて、配信された暗号情報６６を復元し、デバイス６８を通じて再生部６９ａ，６９ｂにより情報が再生される。この再生部６９ａ，６９ｂは、所有物６３に含まれていてもよいし、所有物６３とは切り離されていてもよい。映像配信の場合には、デバイス６８を通じて映像のみ，又は映像と音声とが再生され、音楽配信の場合には、デバイス６８を通じて音楽が再生されることになる。このとき、サービス媒体である所有物６３内には、暗号情報６６が暗号化されたままの状態で保持されるように、サービス媒体に規制を加えることで、所有物６３の情報が不特定の者に流出するのを防ぐことができる。つまり、暗号鍵４３をサービス媒体である所有物と共に購入した情報受信者６１のみがサービスを享受することができる。

【０１５５】この場合、暗号鍵４３がサービス媒体（所有物６３）にはデフォルト値として残らないので、サービス媒体（所有物６３）の貸借に際しても、情報の流出を防ぐことが可能になる。

【０１５６】本実施形態の形態で行われる情報の配信は、サービス媒体である所有物６３の購入のもと、暗号情報６６の配信の際、および暗号鍵４３の配信の際に課金することができる。このように、２系統に情報配信および課金形態を分割することにより、情報著作権を守り、かつ効率的な情報伝送を選択できるので、本実施形態の情報配信システムは配信ビジネスに有用である。

【０１５７】なお、上記各実施形態において、暗号鍵４１，４３がバイオメトリクス情報であってもよい。

【０１５８】

【発明の効果】本発明の認証システム，認証請求装置，検証装置又はサービス媒体によれば、暗号情報の作成に際して時間的に変化する特性を有する変動情報を用いるようにしたので、第三者の盗用のおそれを低減することができる。

【図面の簡単な説明】

【図１】一般的な認証システムにおける認証の流れを模式的に示すブロック図である。

【図２】本発明の第１の実施形態の認証システム全体の構成及び情報の流れを概略的に示すブロック図である。

【図３】本発明の第２の実施形態の認証請求装置の構成を概略的に示すブロック図である。

【図４】本発明の第２の実施形態の携帯端末中の変動情報検出部の構成を示すブロック図である。

【図５】本発明の第３の実施形態ににおける検証装置１６Ｂの構成例を示すブロック図である。

【図６】本発明の第４の実施形態における認証システム

31

の構成を概略的に示すブロック図である。

【図７】本発明の第５の実施形態における認証システムの構成を概略的に示すブロック図である。

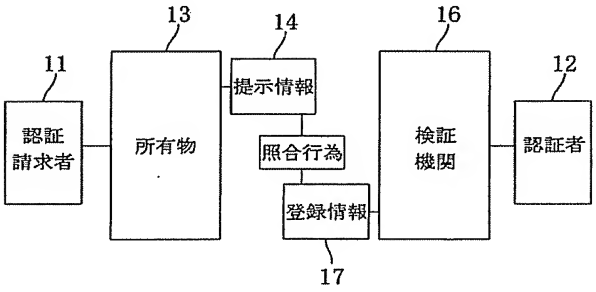
【符号の説明】

１１　認証請求者
１２　認証者
１３　所有物
１３Ａ　携帯端末（認証請求装置）
１４　提示情報
１５　照合部
１６　検証機関
１６Ａ　検証部
１６Ｂ　検証装置
１７　登録情報
３１　情報入力部
３２　固定情報記憶部

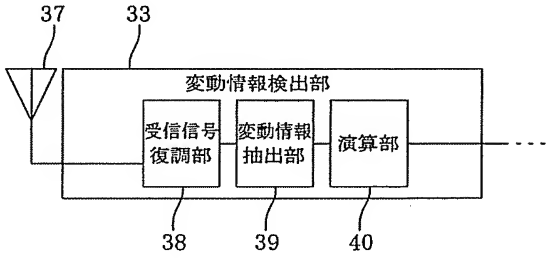
32

３３　変動情報検出部
３４　認証情報演算部
３５　入出力部
３６　情報記録部
３７　アンテナ
３８　受信信号復調部
３９　変動情報抽出部
４０　演算部
４１　暗号鍵（固定情報）
４２　公開鍵（公開情報）
４３　暗号鍵
４４　バイオメトリクス情報（固定情報）
４５　変動情報
４６　暗号情報
４７　変動情報提供者

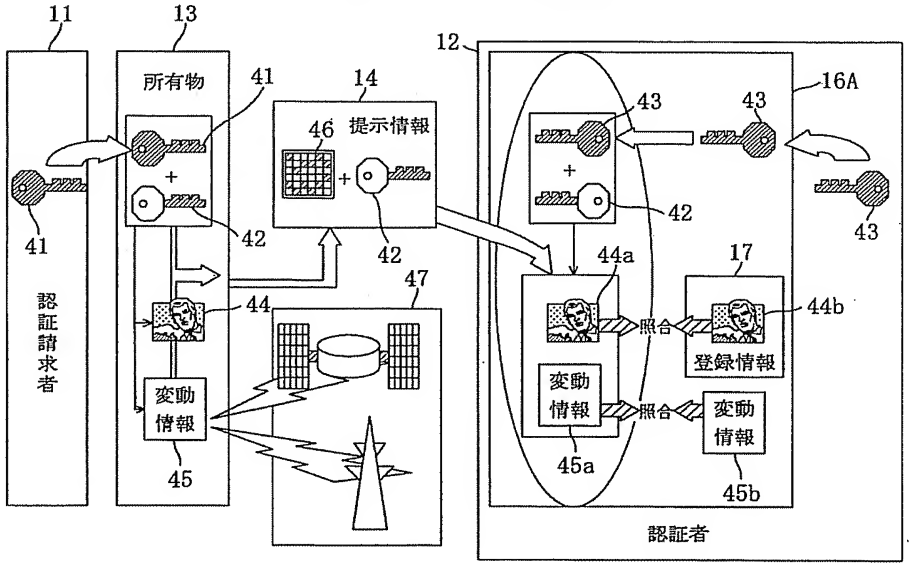
【図１】



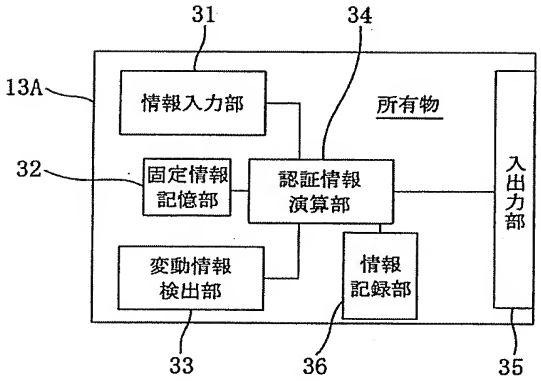
【図４】



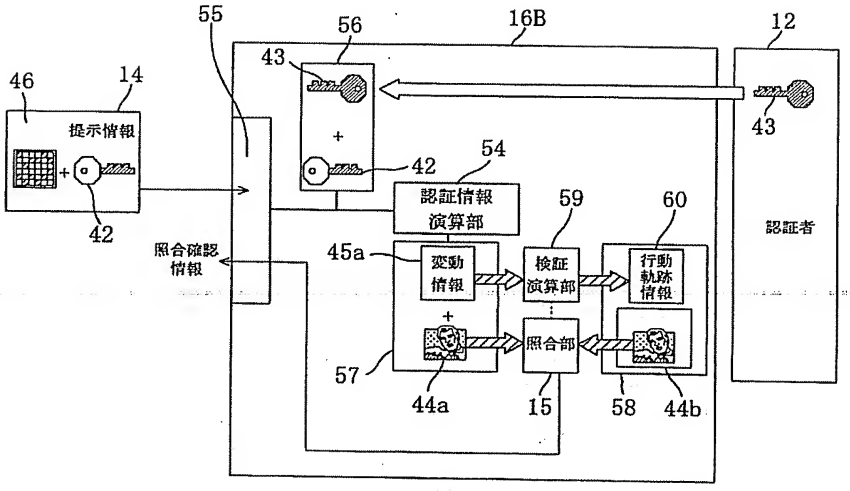
【図２】



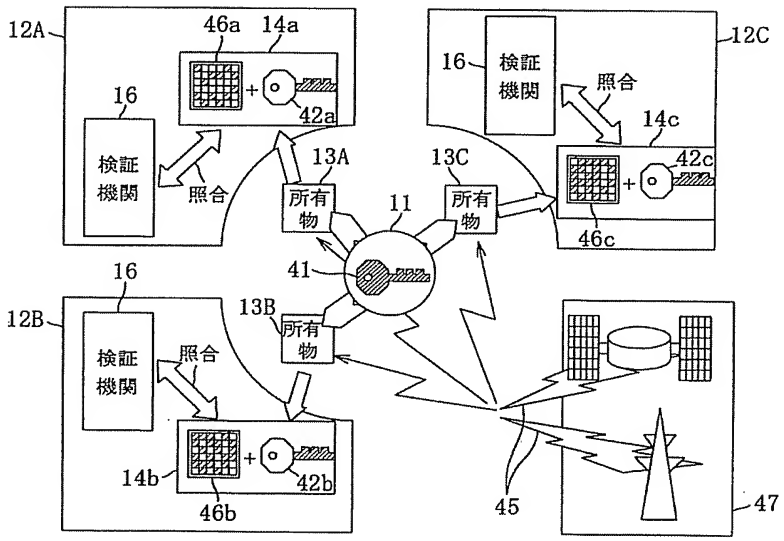
【図３】


31
34
13A
情報入力部
所有物
32
固定情報
記憶部
認証情報
演算部
入出力部
変動情報
検出部
情報
記録部
33
36
35

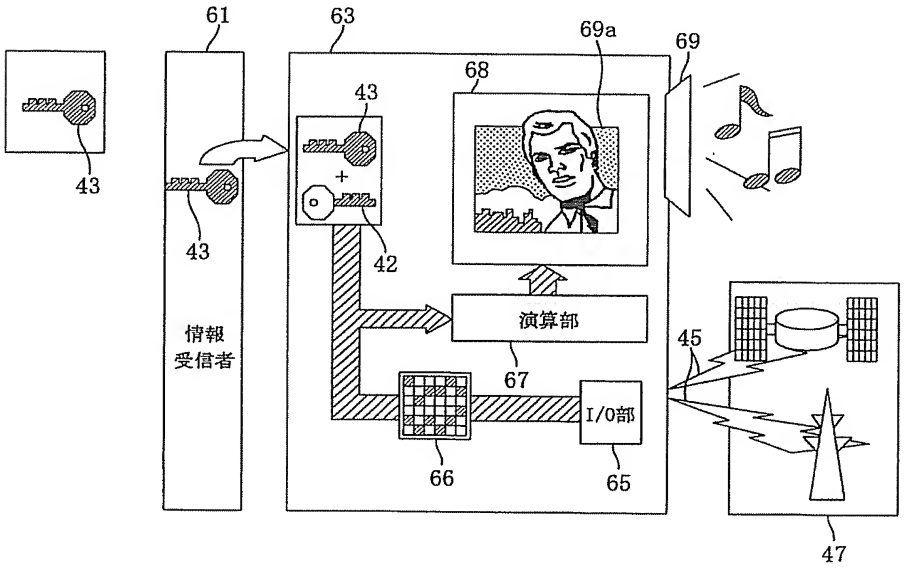
【図５】


55
56
16B
12
43
46
14
提示情報
42
54
認証情報
演算部
59
60
照合確認
情報
45a
変動
情報
検証
演算部
行動
軌跡
情報
照合部
認証者
57
44a
15
58
44b

【図６】


12A
46a
14a
42a
16
検証機関
照合
13A
所有物
11
13C
所有物
16
検証機関
照合
12C
14c
42c
46c
41
16
12B
検証機関
照合
13B
所有物
14b
42b
46b
45
47

【図７】


61
63
69a
69
68
43
43
43
42
情報受信者
演算部
67
I/O部
66
65
45
47